RESEARCH ARTICLE

Improved Signcryption Algorithm for Information Security in Networks

R. Bhagavath Nishanth
ECE (4th Year), Velammal Engineering college, Chennai-66, India

Dr. B. Ramakrishnan
Associate Professor, Department of Computer Science and Research Centre
S.T. Hindu College, Nagercoil, India.

M. Selvi
Research Scholar, S.T. Hindu College, Nagercoil, India.

Abstract – In a Cryptographic primordial, the functions of the digital signature and the public key encryption are concurrently carried out. To safely communicate incredibly large messages, the cryptographic primordial known as the signcryption is effectively employed. Though a lion's share of the public key based mechanism are appropriate for miniature messages, the hybrid encryption (KEM-DEM) offers a proficient and realistic method. In this document, we are cheered to launch an improved signcryption method, which takes cues from the KEM and DEM approaches. The KEM algorithm employs the KDF approach to summarize the symmetric key. The DEM algorithm makes use of the Elliptic curve cryptography technique to encrypt the original message. With an eye on safety aspects, we have testes three attacks and we are cheered to state that the attackers have failed miserably in locating the safety traits of our improved signcryption technique.

Index Terms – Cryptographic, Signcryption, KEM, DEM, KDF.

1. INTRODUCTION

Of late, the big bang expansion of the mobile computing devices, such as the laptops, personal digital assistants (PDAs) and handheld digital devices has triggered an incredible transformation in the ever-zooming domain of computing. In fact, computing does not attempt to depend entirely on the potential furnished by the personal computers, and the conception of omnipresent computing has surfaced and emerged as one of the hot investigation topics in the unfathomable horizon of computer science [1]. In the omnipresent computing scenario, individual users have the facilities to employ, simultaneously a host of electronic platforms which offer them an olive branch to access all the needed data regardless of time and place. [2].

In this regard, the VANETs (Vehicular Ad hoc Networks) and Mobile Ad hoc Network (MANET) are doing their stylish round as the exceedingly mobile wireless ad hoc networks, casting a significant part in the public safety communications and commercial applications. The fundamental function of cryptography is focused on preserving the confidentiality of messages communicated through various public communication channels. With an eye on programming a message in a way as to keep it at bay from the access of an eavesdropper, we elegantly employ the encryption techniques which invariably deploy certain confidential data such as a key [1].

The privacy and legitimacy have emerged as the safety targets which are highly essential for a safe communication by means of an apprehensive channel. The encryption techniques are effectively employed to usher in privacy and the digital signature techniques advocate enforceability [2]. The safety of communications can be effectively offered by the encryption and digital signature which represent the two basic cryptographic systems. In fact, till last decade, they were deemed as the not worthy and distinctive building blocks of several cryptographic techniques [3].

In the public key systems, a conventional technique digitally signs a communication accompanied by an encryption constituting the signature-then-encryption which is found plagued by two hassles such as the inferior efficacy and the elevated expenses of the related summation, and the incompetency of any random technique to provide the necessary safety. In this regard, the signcryption constitutes a reasonably novel cryptographic approach which in a single coherent stroke successfully performs the functionalities of digital signature and encryption, thereby saving an incredible amount of the computational overheads and communication expenses vis-à-vis the time-honored signature-then-encryption system. Zheng [4] was credited with launching the debut digital signcryption technique which handed on a platter the twin fruits of secrecy and verification in a single sound step coupled with the condensed computational cost and communication expenses compared to the sign then encrypt

(StE) or encrypt then sign (EtS) method. Thereafter, a host of signcryption systems have been spearheaded [2].

With the intention of carrying out confidentiality communication for bulky messages, the hybrid encryption approach can be effectively applied which divides the encryption endeavor into two segments. While the former component exploits the public key methods to encrypt a one-time symmetric key, the latter is entrusted with the task of deploying the symmetric key to encrypt the real message. In this novel brand of configuration, the public key module of the technique is labeled as the Key Encapsulation Mechanism (KEM) and the symmetric key module termed as the Data Encapsulation Mechanism (DEM) [5].

Cramer and Shoup [6, 7] competently conceived a convincing model where the asymmetric and symmetric segments of the cryptosystem were properly segmented into an asymmetric KEM and a symmetric DEM. In their documents, they elegantly envisioned a separate security standard for the KEM and the DEM carrying the conviction that the completion of the criteria certifies the complete confidentiality for the entire encryption technique. Dent [8] deftly discharged the duty of developing the innovative model to the signcryption setting by green-signaling an innovative safety benchmark for both the KEM and the DEM. Further, the entire preceding creations for the certificate-free cryptosystems were conceived on the basis of the bilinear coupling [9-11].

Beak et al [10] displayed the brilliance of brightly bringing to limelight the debut certificate-free cryptosystem devoid of the bilinear coupling. Generally, the certificate-free cryptosystem is susceptible to the key substitution menace, in view of the fact that in the absence of proper certification of the public keys, it has the effect of giving carte-blanche to any unscrupulous ambusher to the unauthorized substitution of the public key of any authentic user in the system. Thus, the daunting dilemma staring starkly at the face while envisaging the design of certificate less cryptosystem is to usher in an appealing system which is well-equipped with ample safety even in the emergent case of substitution of the public key of the user. The outstanding investigation by Dent [12] furnished an all-inclusive outline of the design of provably safe certificate-free encryption mechanisms [13].

2. RELATED WORKS

Xin Huang et al. [14] excellently explored the eventuality of employing the human intuitive channel as a segment of the BSN applications. In this regard, the legally outlined HH and HD channels were able to furnish the validity and honesty of data exchange. They were likely to be fruitful for the purpose of safeguarding data exchanged over DD channel which were trapped, expunged, or adapted by the aggressor. Furthermore, they elegantly launched a gathering responsibility convention model. The human-intelligent channels-based gathering duty conventions were also subjected to scrutiny, exploring the feasible ambushes and suggesting the antidotes. In addition, the salient features of the ECDH-SHCBK and ECDH-HCBK were thoroughly recounted. Further the MITM ambushes, which caused the greatest threat to the ECDH, were totally annihilated.

It was Gang Yu In Ji *et.al.* [`5] who initially offered an innovative safety model for identity based generalized signcryption which sparkled with the added qualities of absoluteness when compared to the modern model. Subsequently, they gave vent to an identity based generalized signcryption mechanism, followed by the introduction of the safety verification of the novel technique in the entire model. The new-fangled technique was able to offer incredibly reduced performance intricacy vis-à-vis that of the modern identity based generalized signcryption. Further, the novel technique was at par with the current standard signcryption systems in terms of the computation complications.

Nadia M. G. Al-Saidi [16] climbed up the noble ladder of success when they signaled a commonly composed signcryption plan utilizing the compression capability of a fractal encoding and decoding strategy. In their document, the message is instantaneously encrypted by means of an expert encoded stratagem, accompanied by the configuration of a secure and sophisticated digital signature with the mighty help of the hash function. Thereafter, the fractal codes of a digital signature are supplemented to the programmed message intended for communication, giving birth to the positive backdrops of the fractal image coding (FIC). The hash function is expounded for the attained programmed message, after the completion of the decryption task at the receiver's end. With the intention of identifying the grandeur of the message, the attained and the determined has functions are built up to arrive at the check process. The message is identified on the availability of a confirmation mechanism; otherwise, it is shunted down to oblivion. With an eye on effectively exhibiting the fact that the innovative plan is well-geared to generate essential safety needs, it is tested and scrutinized on a war-footing.

In their gorgeous initial proposal, Gang Yu In Ji *et.al.* [17] envisioned a safety pattern for identity based generalized signcryption which was exceedingly supreme in relation to the modern model. Further, they went on to envisage an identity based generalized signcryption technique. In addition, in this whole model, the safety proof of the novel method was furnished. The ground-breaking technique glistened with scaled-down performance complication in relation to the modern identity based generalized signcryption approach. Furthermore, the new-fangled technique was able to maintain an identical computation intricacy with the modern standard signcryption systems.

Pengcheng LI *et.al.* [18] Proficiently propounded a well-organized certificate-free signcryption technique. They delved deep in to the design of a further rational adversarial version, equipped with the requisite skills of offering safety against insider attacks and ensuring privacy and legitimacy, and went on to authenticate it sheltered under the arbitrary oracle model. The unique method eliminated the requirement of coupling to signcrypt a message, and entailed just two coupling functions in the designcrypt phase. It was also illustrated without an iota of doubt in the performance evaluation that their masterpiece technique scheme fared incredibly proficient and pragmatic.

Alexander W. Dent *et.al.* [19] amazingly devised a formal treatment of secrecy for identical technique. In their document, they were able to launch novel configurations tailor-made to satisfy their concepts in the random oracle and the standard models. As a consequence, they could demonstrate that rather than Fiat-Shamir signatures, the whole range domain hash signatures achieved only an inferior level of confidentiality.

Subsequently, they investigated the correlation of the confidential signatures to signcryption techniques. In the case of confidential signature methods and high-entropy communications, they envisioned proper safety models for deterministic signcryption techniques for both high-entropy and low-entropy messages, and demonstrated that the encrypt-and-sign was highly protected. In the long run, they were competent to illustrate that it is anybody's reach to de-randomize any signcryption approach in our innovative technique and thereby attain highly secured deterministic system.

3. PROPOSED METHOD OF IMPROVED SIGNCRYPTION ALGORITHM BASED ON ECC

Our ultimate aim is to build the Hybrid signcryption based on KEM and DEM, the KEM is performed based on the Key Derivation Function (KDF) using the secure pseudo random number generation technique. The KEM algorithm is used for transferring the secret symmetric key; to share the secret key the additional key will be required for different cryptographic reason such as encryption process, integrity protection algorithm. For this purpose here, we used the key derivation function to derive secret key from any other key or known information using the secure pseudo-random number functions. The various properties of KDF, functionality of pseudo-random number generator and the key expansion function. In conventional signcryption algorithm, the DEM is performed based on the AES encryption algorithm. In our proposed method, the AES algorithm is replaced by Elliptic Curve Cryptography (ECC).

Figure 1 represents the block diagram of the entire proposed methodology.

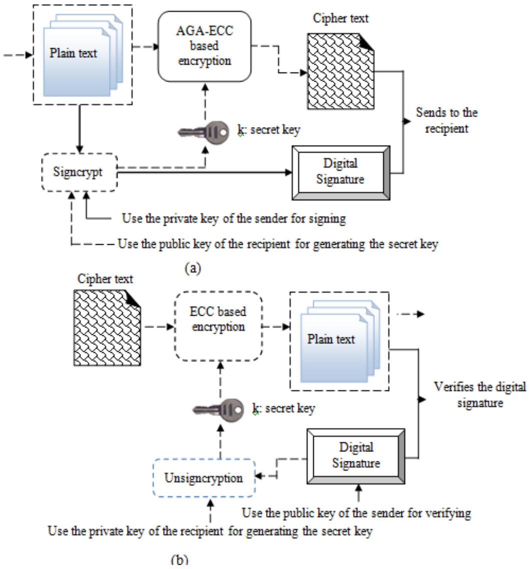

Plain text
AGA-ECC based encryption
Cipher text
Sends to the recipient
k: secret key
Signcrypt
Digital Signature
Use the private key of the sender for signing
Use the public key of the recipient for generating the secret key
(a)
Cipher text
ECC based encryption
Plain text
Verifies the digital signature
k: secret key
Digital Signature
Unsigncryption
Use the public key of the sender for verifying
Use the private key of the recipient for generating the secret key
(b)

Figure 1 Proposed Improved Signcryption algorithm

3.1. Signcryption algorithm

The key generation algorithm: The probabilistic algorithm that takes any two prime numbers $(p,\ q)$ as input and gives the output public key P_k (n,e) and private key S_k (n,d) and symmetric key C_k $(p,\ q)$ Key generation algorithm $\longrightarrow$ (P_k, S_k, C_k).

Data encryption mechanism (DEM): The probabilistic algorithm (AES) that takes original message M and the symmetric key C_k and gives the output ciphertext CM . (M, C_k) Key generation algorithm $\longrightarrow (CM)$.

Key derivation key: The probabilistic algorithm that takes input as an integer n and length of an integer $nLen$ and it gives the output $(z,\ Z)$ where z a random integer is selected from 0 to $n-1$ and Z is $nLen$ string value in the form of most significant bit first which is transformed from z . $(n,\ nLen)$ Key derivation key $\longrightarrow (z,\ Z)$

Encryption: The probabilistic algorithm that takes input random integer z and receiver's public key P_k (n,e) it produces the output $(c,\ C)$ where c is the ciphertext of z and C is $nLen$ string value in the form of most significant bit first which is transformed from c . $(P_k,\ (n,e))$ Encryption $\longrightarrow$ $(c,\ C)$. In our proposed method, this encryption can be done by ECC algorithm.

Key derivation function: The probabilistic algorithm (hashing algorithm (MD5)) that takes input random integer Z and length of the key encryption key $kekLen$ is derived from Z and it gives the output (KEK) key encryption key. $(Z,\ kekLen)$ Key derivation function $\rightarrow (KEK)$

Wrapping function: The probabilistic algorithm (Wrap) that takes input as symmetric key C_k and key encrypting key (KEK) and gives the output wrapped key WK . $(C_k,\ KEK)$ Wrapping function $\rightarrow WK$

Concatenation: The probabilistic algorithm that takes input wrapped key WK , ciphertext C and outputs encapsulated key EK .

Signcryption: The probabilistic algorithm that takes input ciphertext CM , sender's private key S_k (n,d), encapsulated key EK and outputs the signcrypted data (δD). $(CM,\ S_k,(n,d),\ EK)$ Signcryption $\rightarrow (\delta D)$

Unsigncryption process

Signature verification: The probabilistic algorithm that takes input sender's public key $S(P_k)$, signcrypted data δD , and if the produced output will be 1 then the signature is valid else it returns $\perp$ which represents invalid signature. $(S(P_k),\delta D)$ Signature verification $\rightarrow 1\ or\ \perp$.

Detach: The probabilistic algorithm that takes input EK and outputs the wrapped key WK , cipher text C .

Decryption: The probabilistic algorithm that takes input cipher text C the receiver's private key S_k (n,d) it produces the output Z.

Key derivation function: The probabilistic algorithm (hashing algorithm (MD5)) that takes input integer Z and length of the key encryption key $kekLen$ is derived from Z and it gives the output (KEK) key encryption key. $(Z,\ kekLen)$ Key derivation function $\rightarrow (KEK)$

Unwrapping function: The probabilistic algorithm (Wrap) that takes input as wrapped key WK and key encrypting key (KEK) and gives the output symmetric key C_k . $(WK,\ KEK)$ Wrapping function $\rightarrow C_k$.

Data encryption mechanism (DEM): The probabilistic algorithm (AES) that takes ciphertext CM and the symmetric key C_k and gives the output original message M .(CM, C_k) Key generation algorithm $\rightarrow (M)$.

3.2. Elliptic curve Cryptography (ECC)

Encryption

Here in the signcryption algorithm, we have utilize an ECC method for create a private and public key for the encryption. ECC has certain advantages when compared to the other encryption algorithms such as short key, high security, high speed, small storage space and low bandwidth. The private and public keys are generated by the ECC method makes the data more secure for embedding and also the generated keys are robust. The key generation and formation are described below.

ECC Key generation process

The operations of elliptic curve cryptography are defined over two finite fields: Prime field and Binary field. The suitable field is selected with finitely huge number of points for cryptographic operations. Here, we have used prime field operations by choosing a prime number P_{rm} , and finitely large numbers of basic points are generated on the elliptic curve, such that the generated points bp are between 0 to Z . Then, we randomly select one basic point $p_r(R_1, R_2)$ for cryptographic operations and this point satisfies the equation of the elliptic curve on a prime field, which is defined as,

$$v^2 \bmod P_{rm} = u^3 + \alpha u + \beta \bmod\ P_{rm} \qquad (1)$$

Here we are calculating the random point from bp which satisfies the constraint. In Equ. (2), $\alpha\ and\ \beta$ are the parameters that defining the curve, and $u\, and\, v$ are the coordinate values of the generated points bp . We select the basic point p_r to perform the cryptography, we need to select a private key pv_{ky} on the sender side, which is also an optimal integer less than P_{rm} and generate a public key $pu_{ky} = pv_{ky} * p_r$. Now each text T_{xt} has individual private pv_{ky} and public keys pu_{ky} . The private and public values are added and that decimal value is converted into the binary value. Then least significant bit is chosen. This DataStream is used for the encryption of text.

Encryption and Decryption:

The data is encrypted using the ECC technique. The message is encrypted by using ECC and sends that encrypted message to the receiver side. The encrypted message is send in the form of,

$$\gamma = (E_m, C_j) \qquad (2)$$

$$E_m = O_m * p_r \qquad (3)$$

$$q_j = (u,v) + O_m * (S(p_v) * p_r) \qquad (4)$$

In Equ. (2), E_m is encrypted message it is calculated by Equ. (3) i.e. the multiplication of the original message O_m with the basic point p_r and q_j is computed by Equ. (4). In Equ. (4) $S(pv_{ky})$ is the private key of the sender. This message γ is send to the receiver.

4. RESULTS AND DISCUSSION

The proposed methodology for secured data transaction in a network is implemented in Java with user defined network. Some of the screenshots are described as follows:

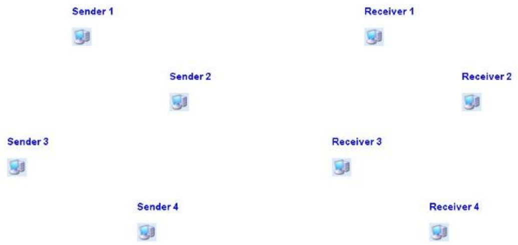
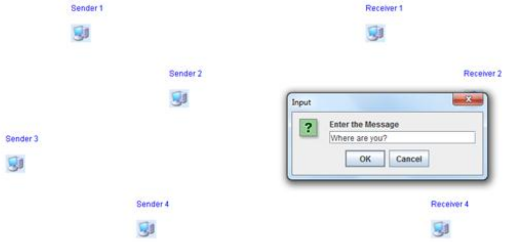


Figure 2 Network representation

Here we organized a network with some nodes in which the data transfer to be held which is presented in Figure 2. Initially the sender node has to select the receiver node to which node the data to be transferred. The sender can transfer the data to any node inside the network in a secured way based on our proposed signcryption algorithm.

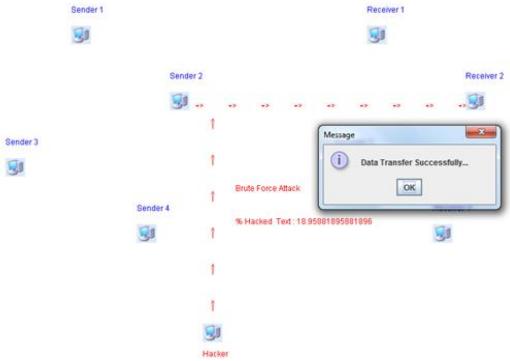


Enter the Message

Where are you?

Figure 3 Data tranfer process

After selecting the receiver node, the sender will tranfer the data or message which is presented in Figure. 3



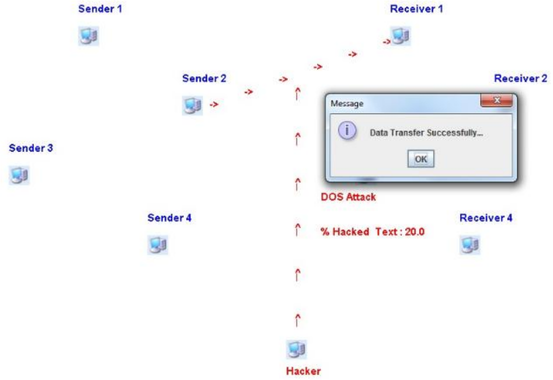
Data Transfer Successfully...

Brute Force Attack

% Hacked Text : 18.95881895881896

Figure 4 Brute Force attack

While transfering the data, hackers or unauthorized node may try to hack the data. We analyzed 3 types of attacks such as DOS, Brute Force and Man In Middle attacks. The Hackers will try to break the secret keys to get the data. In Figure 4, Brute Force is presented and the attacker hacked some data which is 20% similar to the original data. Once the receiver got the message successfully, the it sends the acknowlegement to the sender which is described in Figure 5.



Data Transfer Successfully...

DOS Attack

% Hacked Text : 20.0

Figure 5 The Data transferred to the receiver 1

4.1. Comparative Analysis

Here Table 1 represents the encryption time of various cryptographic encryption algorithm with various lengths. Our proposed ECC algorithm outperforms the existing algorithms in terms of key similarity, encryption time, computational time and key breaking time.

Our proposed security system is analyzed with various attacks such as brute force attack, Daniel of Service (DOS) and Man in Middle (MIM) attack. While using these attacks, the security of the system is evaluated in terms of key breaking time, decrypted text and similarity of the hacked text. The similarity of the hacked text can be analyzed in Table 1.

Algorithm	Similarity (in %)		
	DOS attack	MIM attack	Brute force attack
AES	37.098	22.809	42.848
DES	35.676	21.787	40.897
RSA	29.086	16.6635	31.453
ECC	28.989	13.986	24.678

Table 1 Key similarity

The proposed ECC algorithm encrypts the text in minimum time when compared to the existing algorithm. Here in Table 2, the encryption algorithms are tested with varying length text messages such as “Network” and “Information”. Our proposed algorithm utilizes less time for encryption.

Encryption Algorithm Msg. Length	Proposed ECC	AES	DES	RSA
Length 7 (Network)	272	336	325	315
Length 11 (information)	345	410	401	372

Table 2 Encryption time analysis of various cryptographic algorithms

Figure 6 represents the key breaking time for various encryption algorithm while employing various security attacks. In this, our proposed algorithm is fighting strongly with attacks and the encryption key can be broke after a long time only. Here the key breaking time is better for our proposed algorithm while the others performs less.

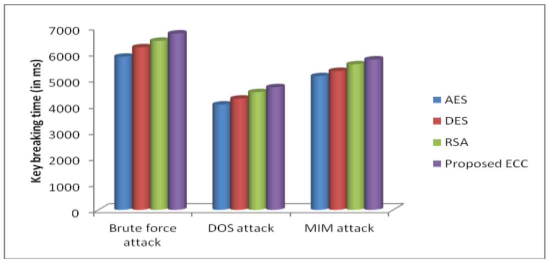


Figure 6 The comparison of key breaking time between proposed and existing algorithms

The computational time is the most important process in the information transaction security. Cryptographic algorithms play a major role in it. The complexity of the algorithm depends upon the encryption time. Here Table 4 describes the computational time of our proposed Signcryption with ECC algorithm with other existing techniques. From the above results we observed that the proposed signcryption scheme outperforms the existing algorithm and leads to the secured data transaction.

Algorithm	Time (in ms)
Existing signcryption algorithm	456
Signcryption with ECC	428

Table 3 Comparison of computational time

5. CONCLUSION

The hybrid signcryption, in essence, takes cues from the KEM and DEM approaches wherein the KEM technique exploits the KDF (key derivative function) method to encapsulate the symmetric key. The KDF, in turn, creates the key encryption key (KEK) to encrypt the symmetric key in accordance with the arbitrary integer and ECC encryption technique. At the receiver end, the designcryption technique processes the signcrypted data and subsequently deploys the KDF approach to locate the key encryption key with the assistance of the private key of the receiver. Later on, the decapsulation procedure extends a helping hand to locate the symmetric key by means of the key encryption key. The decryption procedure is activated on the cipher text to attain the original message as per the symmetric key. It is cheering to the note that in terms of key parameters like the encryption time, key similarity, key breaking time and computational time, our big bang technique scales far higher levels of excellence in performance, pushing to the backyard the peer systems.

REFERENCES

[1] Masayuki Abe, Rosario Gennaro and Kaoru Kurosawa, “Tag-KEM/DEM: a New Framework for Hybrid Encryption and a New Analysis of Kurosawa-Desmedt KEM”, in proceedings of Eurocrypt, pp. 128- 146, 2005.

[2] Sharmila Deva Selvi, S. Sree Vivek, C. Pandu Rangan, "Identity Based Public Verifiable Signcryption Scheme", Proceedings of the 4th international conference on Provable security, PP.244-260, 2010.

[3] Mohsen Toorani and Ali A. Beheshti, "An Elliptic Curve-based Signcryption Scheme with Forward Secrecy" journal of applied science, vol. 9, no. 6, p. 1025-2035, 2009.

[4] Yuliang Zheng, “Digital signcryption or how to achieve cost (signature & encryption) < < cost (signature) + cost (encryption)”, In Advances in Cryptology, CRYPTO - 1997, volume 1294 of Lecture Notes in Computer Science, pages 165–179, 1997.

[5] Fagen Li, Masaaki Shirase, Tsuyoshi Takagi, "Certificateless Hybrid Signcryption", Information Security Practice and Experience Lecture Notes in Computer Science, Vol. 5451, pp 112-123, 2009.

[6] R. Cramer and V. Shoup, “Design and analysis of practical public key encryption schemes secure against adaptive chosen ciphertext attack,” SIAM Journal on Computing, vol. 33, no. 1, pp.167-226, 2004.

[7] Victor Shoup, "Using Hash Functions as a Hedge against Chosen Ciphertext Attack" Advances in Cryptology — EUROCRYPT 2000 Lecture Notes in Computer Science, Vol.1807, pp 275-288, 2000.

[8] Alexander W. Dent, "Hybrid Signcryption Schemes with outsider Security", Information Security Lecture Notes in Computer Science, Vol. 3650, pp. 203-217, 2005.

[9] Joonsang Baek, Reihaneh Safavi-Naini, and Willy Susilo. Certificateless public key encryption without pairing. In Information Security - ISC 2005, volume 3650 of Lecture Notes in Computer Science, pages 134–148. Springer, 2005.

[10] Zhaohui Cheng and Richard Comley. "Efficient certificateless public key encryption. In proceedings of eurocrypt 91, LNCS 547, 2005.

[11] Jong Hwan Park, Kyu Young Choi, Jung Yeon Hwang, and Dong Hoon Lee. Certificateless public key encryption in the selective-id security model (without random oracles). In Pairing-Based Cryptography - Pairing 2007, volume 4575 of Lecture Notes in Computer Science, pages 60–82. Springer, 2007.

[12] Alexander W. Dent, "A survey of certificateless encryption schemes and security models", International Journal of Information Security, Volume-7, no. 5, pp: 349–377, 2008.

[13] S. Sharmila Deva Selvi, S. Sree Vivek, C. Pandu Rangan, "Cryptanalysis of Certificateless Signcryption Schemes and an Efficient Construction without Pairing", journal of Information Security and Cryptology, Vol. 6151, pp 75-92, 2011.

[14] Xin Huang, Bangdao Chen, Andrew Markham, Qinghua Wang, Zheng Yan, Andrew William Roscoe, "Human interactive secure key and identity exchange protocols in body sensor networks", Information Security, IET, Vol:7, No: 1, PP. 30-38, 2013.

[15] Gang Yu, Xiaoxiao Ma, Yong Shen, Wenbao Han, "Provable Secure Identity Based Generalized Signcryption Scheme", Journal of Theoretical Computer Science, vol. 411, no, 40-42, pp. 3614-3624, 2010.

[16] Nadia M. G. Al-Saidi, "An efficient signcryption method using fractal image coding scheme", International Journal of Applied Mathematics and Informatics, vol.6, no. 4, pp.189-197 , 2012.

[17] Gang Yu, Xiaoxiao Ma, Yong Shen, Wenbao Han, "Provable Secure Identity Based Generalized Signcryption Scheme", Journal of Theoretical Computer Science, vol. 411, no, 40-42, pp. 3614-3624, 2010.

[18] Pengcheng LI, Mingxing HE, Xiao LI, Wengang LIU, "Efficient and Provably Secure Certificateless Signcryption from Bilinear Pairings", Journal of Computational Information Systems vol. 6, no. 11, pp.3643-3650, 2010.

[19] Alexander W. Dent, Marc Fischlin, Mark Manulis, Dominique Schröder, Martijn Stam, "Confidential Signatures and Deterministic Signcryption", Proceedings of 13th International Conference on Practice and Theory in Public Key Cryptography, vol. 6056, pp. 462-479, 2010.

Authors

Mr. R. Bhagavath Nishanth is doing his final year Electronics and Communication Engineering at Velammal Engineering College, Chennai. He has authored three research papers in reputed international journals in His research interests include Network Communication, Mobile Network and Robotic Systems.

Dr. B. Ramakrishnan is currently working as Associate Professor in the Department of Computer Science and research Centre in S.T. Hindu College, Nagercoil. He received his M.Sc degree from Madurai Kamaraj University, Madurai and received Mphil (Comp. Sc.) from Alagappa University Karikudi. He earned his Doctorate degree in the field of Computer Science from Manonmaniam Sundaranar University, Tirunelveli. He has a teaching experience of 28 years. He has twelve years of research experience and published more than forty research articles in reputed international journals. His research interests lie in the field of Vehicular networks, mobile network and communication, Cloud computing, Green computing, Ad-hoc networks and Network security.

Mrs. M. Selvi received his B.Sc Computer Science degree from S. T. Hindu college affiliated Manonmanium Sundaranar University, Tirunelveli, India and MCA degree from Anna University, India. Presently she is a research scholar in Department of Computer Science, S. T. Hindu College, Nagercoil, India. She has three years of research experience and authored four research papers in reputed international journals and conferences. His research interests include Data Mining, Information Security, Vehicular Network and Network Security.